IN THE CLAIMS

1 (Previously Presented). A method for use with a computer system, comprising:

receiving a plurality of packets including security packets and non-security packets;

identifying the next security packet to be transmitted;

identifying the next non-security packet to be transmitted;

determining whether the next security packet is ready to be transmitted and, if not, transmitting the next non-security packet and, if the next security packet is ready for transmission, transmitting the next security packet; and

if the next security packet is not ready for transmission, processing the security packet while transmitting the next non-security packet.

Claim 2 (Canceled).

3 (Original). The method of claim 1 including processing said packets in a first in first out memory.

4 (Original). The method of claim 1 including monitoring an input queue and fetching one type of packet to bypass another type of packet for transmission.

Claim 5 (Canceled).

6 (Original). The method of claim 1 including receiving packets to be transmitted in a first in first out memory, checking each packet to determine its security status, and providing a pointer to said packet based on its security status.

7 (Original). The method of claim 6 including organizing a plurality of packets in said first in first out memory as a linked list of packet blocks.

8 (Original). The method of claim 7 including marking each of said packet blocks in said first in first out memory as being either a security packet or a non-security packet.

9 (Original). The method of claim 8 including marking packets as security packets or non-security packets depending on the attributes that are indicated in an internet protocol header associated with each packet.

10 (Original). The method of claim 7 including processing a security packet in an authentication and security engine, and then providing a pointer that points to the security packet.

11 (Original). The method of claim 10 including selecting between pointers to security packets and non-security packets for transmission of said packets from a network controller to a network interface.

12 (Original). The method of claim 11 including selecting from among the pointers based on a round robin priority basis.

Claim 13 (Previously Presented). An article comprising a medium storing instructions that, when executed, enable a processor-based system to:

receive a plurality of packets including security packets and non-security packets;

identify the next security packet to be transmitted;

identify the next non-security packet to be transmitted;

determine whether the next security packet is ready to be transmitted and, if not, transmitting the next non-security packet and, if the next security packet is ready for transmission, transmitting the next security packet; and

if the next security packet is not ready for transmission, process the security packet while transmitting the next non-security packet.

14 (Previously Presented). The article of claim 13, wherein the instructions, when executed, further enable a processor-based system to transmit non-security packets ahead of security packets.

15 (Previously Presented). The article of claim 13, wherein the instructions, when executed, further enable a processor-based system to monitor an input queue and fetch one type of packet to bypass another type of packet for transmission.

Claim 16 (Canceled).

17 (Previously Presented). The article of claim 13 wherein the instructions, when executed, further enable a processor-based system to receive packets to be transmitted in a first in first out memory, check each packet to determine its security status and provide a pointer to the packet based on its security status.

18 (Previously Presented). The article of claim 17 wherein the instructions, when executed, further enable a processor-based system to organize a plurality of packets in a first in first out memory as a linked list of packet blocks.

19 (Previously Presented). The article of claim 18 wherein the instructions, when executed, further enable a processor-based system to mark each of said packet blocks in said first in first out memory as being either a security packet or a non-security packet.

20 (Previously Presented). The article of claim 19 wherein the instructions, when executed, further enable a processor-based system to mark packets as security or non-security packets depending on the attributes that are indicated in an internet protocol header associated with each packet.

21 (Previously Presented). The article of claim 20 wherein the instructions, when executed, further enable a processor-based system to provide a pointer that points to a security packet.

22 (Previously Presented). The article of claim 21 wherein the instructions, when executed, further enable a processor-based system to provide pointers for non-security packets and to select between pointers to security packets and non-security packets for transmission of said packets.

23 (Previously Presented). The article of claim 22 wherein the instructions, when executed, further enable a processor-based system to select among pointers based on a round robin priority basis.

Claims 24-30 (Canceled).